CLAIMS

1. A method for preparing an authenticable and verifiable image of a module, the method comprising:

receiving a module image;

adding to the module image a size and location block;

adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image; and

adding to the authenticable image a verification block that includes a digital signature prepared from the module image.

2. The method of claim 1 wherein adding to the module image a size and location block further includes:

adding, in a specific location, a header that includes an image size, location, and globally unique identifier describes a size and location of the firmware image within a flash memory or other non-volatile memory and that identifies a class of machines for which the firmware module has been created.

3. The method of claim 1 wherein adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image further includes:

adding to the module image an authentication block including an encrypted, hashed module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image.

4. The method of claim 1 wherein adding to the authenticable image a verification block that includes a digital signature prepared from the module image further includes:

adding to the authenticable image a verification block that includes a digital signature prepared by hashing the module image and encrypting the hashed module image with a module-specific private key.

5. Computer instructions that together compose a program that carries out the method of method of claim 1 stored in computer readable medium.

6. A method for authenticating and verifying an authenticable and verifiable module, the method comprising:

extracting, from the authenticable and verifiable module, a module-specific public key and cryptographically protected data related to the module-specific public key;

comparing the cryptographically protected data with the module-specific public key to authenticate the authenticable and verifiable module;

comparing a value calculated from an image, including a size and location block, included within the authenticable and verifiable module a value extracted from a digital signature contained in a verification block within the authenticable and verifiable image to verify the authenticable and verifiable module.

7. The method of claim 6 wherein extracting, from the authenticable and verifiable module, a module-specific public key and cryptographically protected data related to the module-specific public key further includes:

extracting, from an authentication block at a known location within the authenticable and verifiable image, an encrypted, hashed module-specific public key and a clear-text version of the module-specific public key.

8. The method of claim 7 wherein comparing the cryptographically protected data with the module-specific public key to authenticate the authenticable and verifiable image further includes:

hashing the clear-text version of the module-specific public key to produce a newly hashed module-specific public key;

decrypting the encrypted, hashed module-specific public key using a first private encryption key; and

comparing the decrypted, hashed module-specific public key with the newly hashed module-specific public key.

9. The method of claim 8 wherein, when the decrypted, hashed module-specific public key is identical to the newly hashed module-specific public key, the authenticable and verifiable image is determined to be authenticated.

10. The method of claim 6 wherein comparing a value calculated from an executable image, including a size and location block, included within the authenticable and verifiable image a value extracted from a digital signature contained in a verification block within the authenticable and verifiable image to verify the authenticable and verifiable image further includes:

hashing an executable image, including a size and location block, included within the authenticable and verifiable image to produce a newly hashed image;

extracting a digital signature from a verification block within the authenticable and verifiable image, and decrypting the digital signature using the module-specific public key to produce an extracted hashed image;

comparing the extracted hashed image to the newly hashed image.

11. The method of claim 10 wherein, when the extracted hashed image is identical to the newly hashed image, the authenticable and verifiable image is determined to be verified.

12. The method of claim 6 employed during secure access, execution, and/or incorporation of the authenticable and verifiable image into a secure-computer processing environment, wherein, when the authenticable and verifiable image is authenticated and verified by the method of claim 6, the authenticable and verifiable image is accessed, executed, and/or incorporated, and when the authenticable and verifiable image is not authenticated or not verified, the authenticable and verifiable image is not executed and/or incorporated.

13. The method of claim 12 employed in the secure booting of a secure computer system, wherein, when an authenticable and verifiable image is not executed and/or incorporated, the secure boot fails.

14. Computer instructions that together compose a program that carries out the method of method of claim 6 stored in computer readable medium.

15. An authenticable and verifiable image of an module stored in a computer-readable medium comprising:

a module image, including a size, location, and globally unique-identifier block;

an authentication block; and

a verification block.

16. An authenticable and verifiable image of an module of claim 15 wherein the authentication block contains an encrypted, hashed module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image.

17. An authenticable and verifiable image of an module of claim 15 wherein the verification block that includes a digital signature prepared by hashing the module image and encrypting the hashed module image with a module-specific private key.

18. A method for preparing an authenticable and verifiable image of a module, the method comprising:

a module-image receiving step;

a size-and-location-data adding step that adds size-and-location data to the received module image;

an authentication-adding step that adds, to the module image, authentication information including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key; and

a verification-block-adding step that adds a digital signature prepared from the module image to the module image.